CHAPTER 2

SYSTEM CONTROLS

CONCEPTUAL FRAMEWORK

A. INTRODUCTION

1. This chapter presents a conceptual framework for instituting and maintaining information system controls. The control framework consists of three elements:

a. Control requirements - the terms used to explain why controls are needed and/or what their implemental ion is expected to achieve.

b. Selection and use of control techniques - the definition, selection, and use of control techniques to satisfy the requirements specified.

c. Areas of control - the terms used to describe how and where control techniques are applied to satisfy basic cent rol requirements.

2. The basic structure of the conceptual framework revolves around these three elements. The remainder of this chapter provides a detailed discussion of the framework and its various supplements. As an aid to the reader, a road map of the system control framework can be found in Figure 2-1 on page 2-4.

3. Most control-related activities have traditionally centered on internal control reviews, risk assessments , and audits of existing automated systems and processes. While these types of reviews are needed, they do not necessarily ensure that adequate management controls are built into current and future systems. Additionally, much of what is written for both managers and systems developers is based on the theoretical aspects of controls. The situation existing today can be summarized as follows:

a. Numerous directives require controls over automated systems, and, while they vary in terminology, specificity, and origin, they all have the same basic objectives. These direct ives point out a need for secure and reliable systems. In spite of these directives, there are a few simple, clear guidelines on how to build controls into a new automated information system and at the same time show compliance with the directives.

b. There are no formal methods currently in use to easily identify needed controls as systems are being developed. As a result, extensive control reviews are needed after the system becomes operational. These reviews are costly and may not result in needed corrective actions. To retrofit, the needed adjustments can cost 50″ to 100 times more than building the controls into the system as it is being developed.

c. There is no controls process defined that is compatible with, and an integral part of, the total systems process. Rather, there is a tendency to address control issues separate from the many other systems activities.

d. Control and security responsibilities are often assigned to personnel who are organizationally remote from systems development and operation. Although some centralized direction on controls is beneficial, the individuals who understand the requirements and the system must play a major role in the controls development process. To do this, a controls methodology is needed to integrate a controls process into all the many other systems-related activities.

4. Fundamentally, automated information systems are developed to support managers to effectively fulfill their responsibilities. In the Federal Government, automated information systems perform a wide range of functions that include: making benefit payments; collecting receivables; and recording and accounting for obligations, costs, revenues, and expenses. In many cases, these kinds of functions are almost completely dependent on automated information systems, thereby creating many new concerns and risks for management. System risks might, for example, result from the following circumstances:

a. An automated system might allow an individual to circumvent the “separation of duties” control instituted in manual systems.

b. When the information trail is automated (i.e., when all support for payment is in machine form), the “process” may be difficult or impossible to monitor.

c. There is a natural, but totally unfounded, tendency to believe that computer-generated output is correct.

5. To address these concerns, managers who operate or use ADP systems should take actions to eliminate or at least reduce the risks to acceptable levels. All such actions taken to reduce risks are referred to as “control techniques” or, more commonly, “controls.” The underlying requirement of control over an automated information system is to provide reasonable assurance that the information processed by the system is reliable and properly safeguarded.

6. Management oversees and effects the development, implementation, and use of automated information systems through a variety of mechanisms, including standards, budget and

procurement review and authorization, and personnel-hiring practices. While existing mechanisms have worked with varying success to ensure that systems support an organization’s mission, they have not always provided reasonable assurance that a system is safe. Systems may improve accuracy, increase productivity, or speed service but at the same time be subject to fraud, waste, and abuse.

B. SYSTEM CONTROL REQUIREMENTS

1. Control requirements are established to address a known vulnerability or promote reliability or security of a system. They can be based on management experience, vulnerability assessments, other reviews, and/or common sense. Regardless of why established, control requirements should be as specific as possible and stated in clear, understandable terms.

2. Four categories of control requirements surfaced in an analysis of the provisions of the system control directives listed in Table 2-1 on page 2-10. These are application controls, general controls, administrative controls, and required system functions. While the ongoing discussion deals with these four categories of control requirements, it should be recognized here that the operational implementation of a controls program will involve a refining of these requirements into sub-requirements or control objectives.

3. The first category, application controls, are those that help assure that information processed is authorized, valid, complete, accurate, and timely. It also contains requirements that ensure that the system is secure and that an audit trail exists.

4. Compliance with the requirements for application controls has proved the most elusive for management to meet. Requirement terminology varies among the many directives, but the intent is the same in all.

5. Three principles are important to note:

a. How information should be handled, once its sensitivity and/or classification has been determined, is fairly well established by the regulating agency.

b. The determination of the classification levels for systems and data is a management responsibility of the sponsoring agency.

c* Once the classification levels are determined by management, the determinations should be systematically applied, and management should be aware of any exceptions.

FIGURE 2.1 -CONTROL FRAMEWORK

CONTROL REQUIREMENTS

Application Controls
- information authorized
- information valid
- information complete
- information accurate
- information timely
- system secure
- system auditable

General Controls

Administrative controls

Required system functions

SELECTION AND USE OF CONTROL TECHNIQUES

Types of controls
- detective
- corrective
- preventive

Characteristics of effective controls
- have a clear purpose
- developed in partnership
- cost-effective
- documented
- tested and reviewed
- manageable

AREAS OF CONTROL

- input
“ output
- processing
- storage
- communications

6. What the third principle means is that sensitive data in a computer data base should have the same classification as they are given in a hard copy publication. Most processes (accounting or otherwise) consist of both manual and automated portions. Reviews of the process should assess the totality of the process components affected, not just a portion of the affected components. Further, management must be aware that increases in security are almost always accompanied by increases in cost, although some security measures can be implemented with little effort. Management must be aware of situations when resources are insufficient to provide the level of protection required, because it is management that must accept the risk of loss and/or disclosure. Because of the terminology and technical complexities of automated processes, the evidence suggests that managers often delegate these critical decisions to their program and/or technical staff. It is of paramount importance that managers fully understand the need for controls, the resource implications of-controls, and the risks associated with inadequate controls. These are management's responsibilities and cannot be delegated.

7. The second category, general controls such as cost-benefit analysis and certification, are quantifiable and require a product to be created for management review and/or acceptance. These tools are essential to good management in the development and operation of systems by facility managers, users, systems analysts, and computer programmers. Another essential tool which should be applied by all managers and users is agency record and disposition schedules.

8. The third category, administrative controls such as supportive attitudes or competent personnel, are generally difficult to quantify and have not resulted in the past in tangible work products within automated information systems.

9. Many of the requirements have become standard operation procedures in some Federal Agencies, with considerable guidance provided on how they should be met.

10. The last category of control requirements, required systems functions, consists of mandated features that must be designed and built into a system, such as a particular access capability.

C. SELECTION AND USE OF CONTROL TECHNIQUES

1. Control techniques are procedures used to meet control requirements. Control techniques employed might be preventive, detective, corrective, or a combination of the three:

a. Preventive controls are put in place to prevent or deter any undesired event. Placing a terminal in a locked room, for example, prevents access to that equipment from personnel without a key.

b. Detective controls are designed to alert management that an undesired event has occurred. An alarm that sounds if the door is forced open, for example, is a detective control.

c. Corrective controls are used in conjunction with detective controls to recover from the consequences of the undesired event. Having insurance to pay for the stolen terminal or a guard force to catch an intruder would be examples of corrective controls.

2. The selection of a control technique should, in most cases, be a group decision to ensure that it is feasible for the entire system, is understood by all affected, and comprehensively meets the organization's control requirements. For example, a user might have to key in special data, operations personnel may have to review exceptions, and a programmer might have to develop codes to be used, because controls can affect many groups associated with the system.

3. Further, the control selected must be cost-effective. (Determining cost-effectiveness for more obvious controls, such as input editing, is usually not an issue.) Controls that require manpower, such as integrity reviews of transactions, can be costly and require a cost-benefit analysis. This analysis becomes part of the controls documentation. Decisions on some controls may also require detailed knowledge of controls already in place. This is especially true of routine controls, such as access controls. The composition of current access controls may greatly affect the design of any additional access controls being contemplated for a particular system.

4. The installation of controls must be accompanied by an effort to provide assurance that the control operates as initially intended. Testing is needed before the control is implemented, as well as later, to be sure it still fulfills the control requirement. Ongoing reviews might be a part of a management initiative. The testing, review schedules and methods are management prerogatives, although external reporting needs would be a consideration. For example, management might decide that test transactions should be reprocessed yearly, while a detailed review of controls documentation should be done each 3 years to coincide with any external reporting requirements specified by OMB Circular A-130 (referenced (e)).

5. The controls selected and implemented must have certain characteristics to ensure that they are effective. They must be:

a. Clear in purpose - If not understood, controls may not be used and if they do not have a clear purpose or address a known vulnerability, they are of little or no value.

b. Coordinated - Developed in partnership by personnel knowledgeable about the application, process, computer systems, and control techniques. It is unlikely that effective, feasible controls can be selected and implemented unilaterally by, for example, a user, a system analyst, a programmer, or an auditor.

c. Cost-effective - The cost of the control should not, in general, exceed the expected benefits. Stated another way, there should be reasonable assurance that the system is protected from a known risk. If total assurance of control were possible, it would probably be prohibitively expensive. More simply, spending $100 to protect against an $80 loss makes little sense.

d. Documented - The documentation process should be simple, understandable, clearly link risks to controls, and provide management with assurance that all reasonable controls are in place. Without some form of documentation, there is no assurance that all known vulnerabilities are addressed or that controls are in place.

e. Tested and reviewed - There must be assurance that the controls function as originally intended. This assurance is needed when the system first becomes operational and also during ongoing operation. Initial controls testing should normally be done when all other aspects of the system are tested. Ongoing testing and review might be done as a part of a general system review, an internal control review, an audit, or other management initiative.

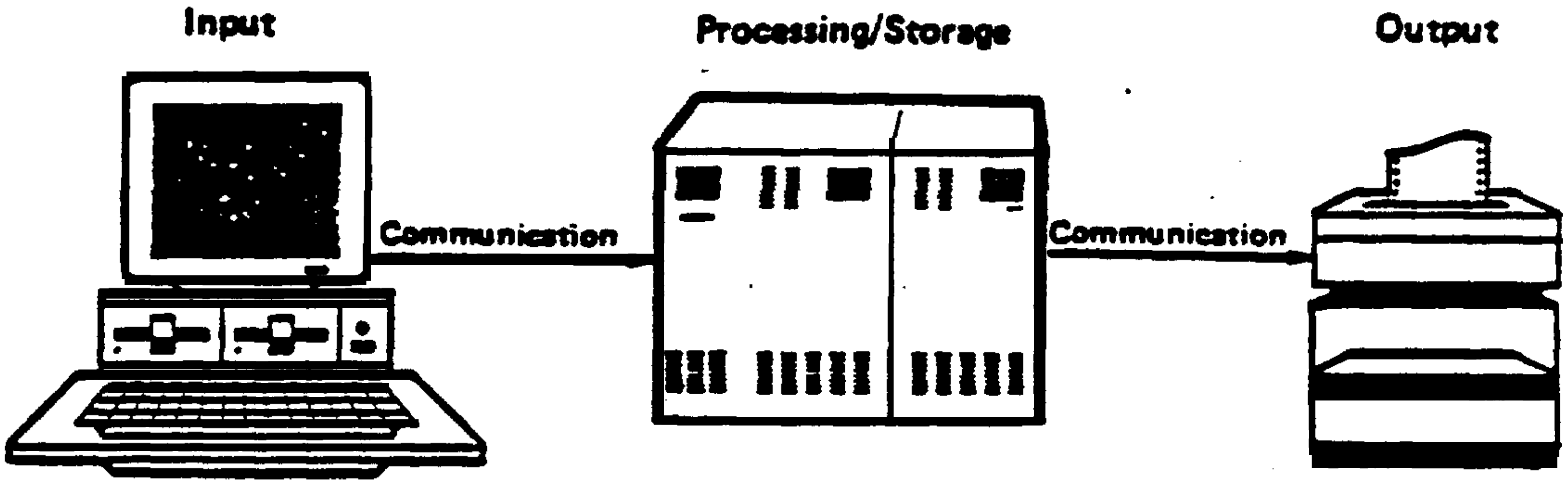
f. Manageable - Management must have the means to change, delete, evaluate cost, upgrade, or review the system of controls under its purview.

D. AREAS OF CONTROL

1. Automated information systems typically encompass data files, computer programs, and equipment, all of which may affect controls in some way. Part of the problem in dealing with controls is the wide variability in how systems are defined. If there was uniformity in definitions, then control techniques could be applied, evaluated, and cataloged more easily.

2. The five control areas listed below are the basic control requirements. These areas, as show in Figure 2-2 on page 2-8, are labeled using traditional terminology.

FIGURE 2-2 - THE FIVE CONTROL AREAS OF A SYSTEM



It is desirable to apply the controls process to one area at a time. This makes the process more manageable, and it also allows *similar* control issues to be addressed collectively. The control areas are:

a. Input - includes the records (also referred to as either manual data or transactions) to be processed by the system, and the associated processes from origination to the computer.

b. output - includes the records and reports produced by the system, and the associated manual processes from the computer to the user.

c. Processing - includes all computer processing to receive the input and store and/or otherwise manipulate the input to produce output.

d. Storage - includes all computer program code and/or instructions and data files.

e. Communications - includes the transmission of data and/or information either between sites or between peripherals at a site.

3. Viewing a system in its pieces makes it easier to set specific control requirements and select control techniques. It is important to retain a system's perspective, to avoid over-control, and to deal with systemwide issues. The following systemwide control issues need to be considered:

a. Control techniques in one control area may lessen the need for controls in another control area; for instance, tight controls over data files may negate the need for some communication controls.

b. Some aspects of a system may require special systemwide attention; e.g., a highly-sensitive subfile may require tight controls during inputting, storage, or outputting.

4. This perspective should be the responsibility of individuals or a group that is involved in all aspects of the system. A user group or a controls specialist assigned to the project might be assigned controls responsibility.

5. In general, the framework proposes that control techniques be applied to defined control areas to fulfill control requirements as illustrated in Figure 2-3.

FIGURE 2-3-MANAGEMENT'S BASICTASKS INDEVELOPING SYSTEM CONTROLS

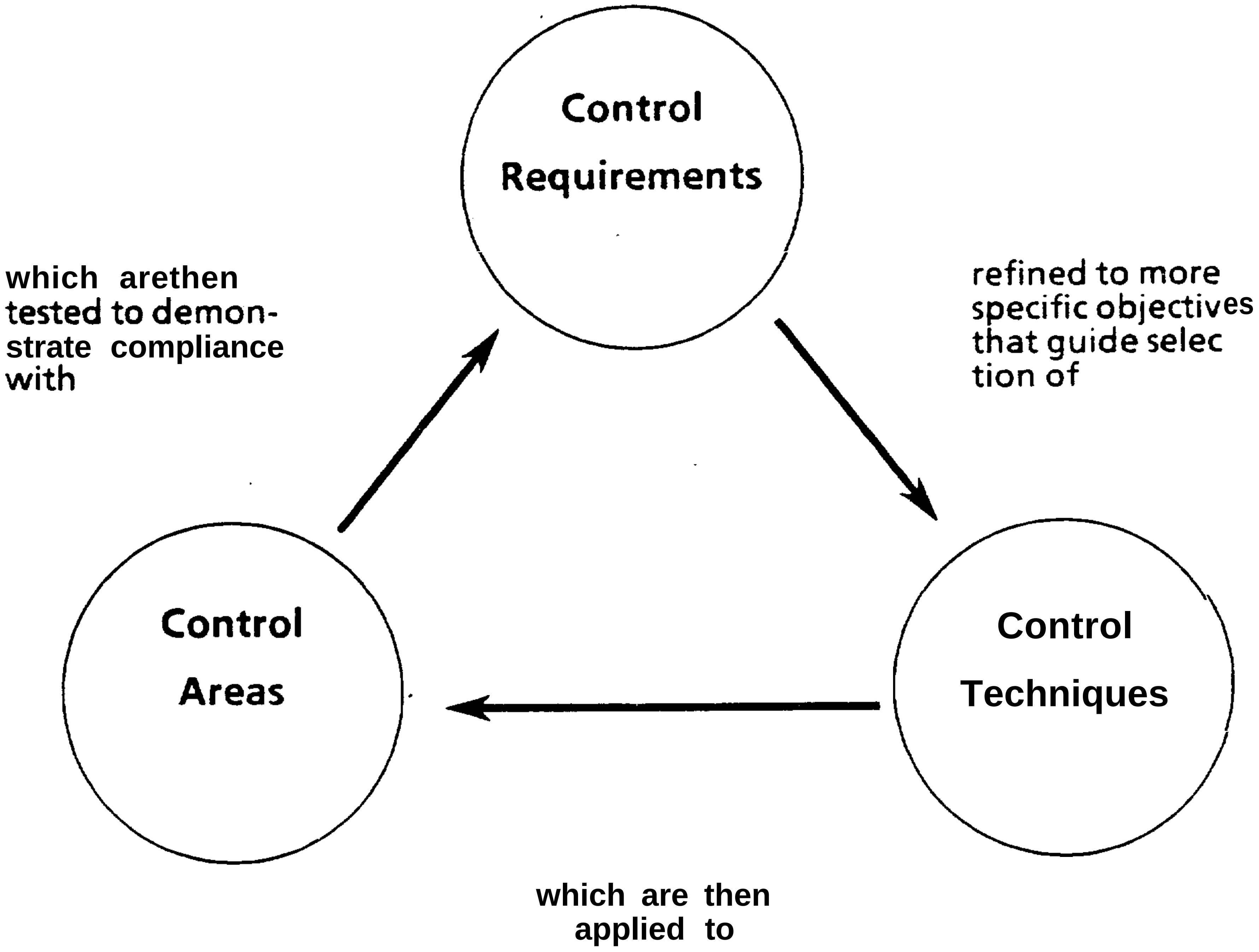

Control Requirements
refined to more specific objectives that guide selec tion of
Control Techniques
which are then applied to
Control Areas
which arethen tested to demon-strate compliance with

TABLE 2-1- MAJOR SYSTEM CONTROL DIRECTIVES

DOCUMENT DATE	DOCUMENT TITLE
OMB	
12/82	Office of Management and Budget, Internal Control Guidelines (reference (h))
12/84	Office of Management and Budget, Circular A- 127, "Financial Management Systems" (reference (d)]
12/85	Off ice of Management and Budget, Circular A-130, "Management of Federal Information Resources" (reference (e))
8/86 Rev.	Office of Management and Budget, Circular A-123, "Internal Control Systems" (reference (c))
DOD	
6/83	Department of Defense Directive 7740. 1,"DoD Information Resources Management Program" (reference (g])
4/87	Department of Defense Directive 5010.38,'' Internal Management Control Program" (reference (f))
GAO	
11/84	General Accounting Office, Policy and Procedures Manual for Guidance of Federal Agencies, Title 2 - "Accounting" [reference (i))
10/84	Appendix 1, "Accounting Principles and Standards" (reference (j))
10/84	Appendix II, "Standards for Internal Controls in the Federal Government" (reference (k))
PL	
1974	Public Law 93-579,"Privacy Act of 1974, " 5 U.S. Code 552a (reference (l))
9/82	Public Law 97-255, "Federal Managers' Financial Integrity Act of 1982, " 31 U.S. Code 66a (reference (b))